REMARKS

Reconsideration and allowance of the subject application are respectfully requested. Claims 1-14 remain pending.

In the Office Action, claims 8-11 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. This rejection is respectfully traversed. Specifically, Applicant respectfully submits that claims 8-11, which recite a computer program product to be executed in a client station, are in compliance with the Guidelines and case precedent as set forth in MPEP § 2106. Nevertheless, to advance prosecution, minor editorial amendments are being made to independent claim 8 to clarify that the computer program product is on a recordable medium and comprises instructions for controlling a client station, which clearly meets the requirements for statutory subject matter as set forth in the Guidelines. Accordingly, Applicant respectfully requests that the Examiner withdraw this rejection.

In addition, claims 1-14 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,424,718 to Holloway in view of published U.S. Patent Application No. 2004/0103316 to Gehrmann. This rejection is respectfully traversed. Specifically, as discussed in more detail below, Applicant respectfully submits that unlike the claimed embodiments of the present invention, the Holloway patent teaches a data communications system employing public and private keys for use by a client, but which are also stored on a server. In other words, the client sends the private key to the server. On the other hand, according to the embodiments of the present invention, a client station uses the private key and destroys the private key after use, and does not forward the private key for storage at, for example, a server. The Gehrmann patent, which is being cited for allegedly teaching the formatting of a signature at a client station, does not make up for these deficiencies in the teachings of the Holloway patent.

The embodiments of the present invention and the teachings of the cited references will now be discussed in more detail.

As described throughout the present application, the embodiments of the present invention provide a system, method and software program for applying an electronic signature from a client station in a network. To accomplish this, the client station is authenticated at a server of the network, and thus establishes an authenticated communication channel between itself and the server. The client then can generate a private key/public key pair, and send to the server, via the authenticated channel, a request for a signature certificate, generated by at least the public key. It should be noted that as described beginning at page 13, line 15 of the present application, the request can provide to the server information pertaining to at least the public key. However, it can be understood from the present application that the client does not share the private key with the sever.

Upon receiving the request, the server sends a signature certificate to the client station, via the authenticated channel. The client station can then calculate a cryptographic signature based on the private key, and then destroys the private key. The client station then formats the calculated signature based on the signature certificate received from the server via the authenticated channel.

The features described above are recited in amended independent claims 1, 8 and 12.

In the rejection, the Examiner admits that the Holloway patent fails to teach or suggest the signature formatting feature as recited in independent claims 1, 8 and 12. Nevertheless, the Examiner relies on the teachings of Gehrmann, and contends that one skilled in the art would have found it obvious in viewing the teachings of Gehrmann to modify the Holloway system to include signature formatting and thus achieve the claimed embodiments of the present invention. Applicant respectfully disagrees.

As discussed briefly above, the Holloway patent teaches a data communications system employing public and private keys for use by a client. As identified by the Examiner, column 3, lines 44-47 and column 4 of the Holloway patent teach that an encrypted private key is stored on a server and downloaded to a client, which performs cryptographic key processing on a message using the decrypted private key. As explained, in particular, in column 4, lines 29-32 of Holloway, the client also sends the encrypted private key and public key to the server for storage.

On the contrary, the embodiment of the present invention manage the public and private keys such that the private key is maintained by the client and destroyed after use, not sent to a server for storage. The private key enables the client to create certificates of relatively short lifetime as described on page 9, lines 23-25 of the present application, and avoids the use of signature keys on a server as described on page 6, lines 10-15 of the present application. In other words, after the authentication process, the server can certify the public key based on the information in the request that the client sends to the server, and send the certificate back to the client based on this public key information. The server does not need the private key information to provide the certificate.

Accordingly, Applicant submits that not only does the Holloway patent fail to teach or suggest signature formatting as identified by the Examiner, but the Holloway patent also fails to teach or suggest that the private key is kept by the client and not provided to the server.

With regard to the teachings of Gerhmann, Applicant respectfully submits that paragraph 0020 of this reference, which is relied upon by the Examiner, does not teach that a server provides a certificate to a client that then uses this certificate to format a signature. Rather, this paragraph states that the client "might also return a certificate containing the public key that can be used by the service to verify signatures made by the client."

Accordingly, in the Gerhmann system, the certificate is being provided by the client, not the server. Moreover, paragraph 0019 of Gerhmann teaches that in the Gerhmann system, the client uses the certificate to authenticate a downloaded code. Again, nowhere does Gerhmann teach *formatting* a signature using a signature certificate.

Applicant further respectfully submits that both references fails to teach or suggest the specific aspects of the processing or the features of the keys or certificates as defined in more detail in the dependent claims.

For all these reasons, Applicant respectfully submits that one skilled in the art would have not found it obvious or possible to achieve the embodiments of the present invention even as defined in independent claims 1, 8 and 12 based on the teachings of the Holloway and Gerhmann references. Hence, all claims should be allowable.

In view of the above, it is believed that the application is in condition for allowance and notice to this effect is respectfully requested. Should the Examiner have any questions, the Examiner is invited to contact the undersigned at the telephone number indicated below.

Respectfully submitted,

Brian C. Rupp, Reg. No. 35,665
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No. 08968

Date: March 7, 2007

CERTIFICATE OF MAILING

I hereby certify that this RESPONSE TO OFFICE ACTION OF DECEMBER 7, 2006 (along with any documents referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: March 7, 2007

I. Mikitiouk

Irina L. Mikitiouk